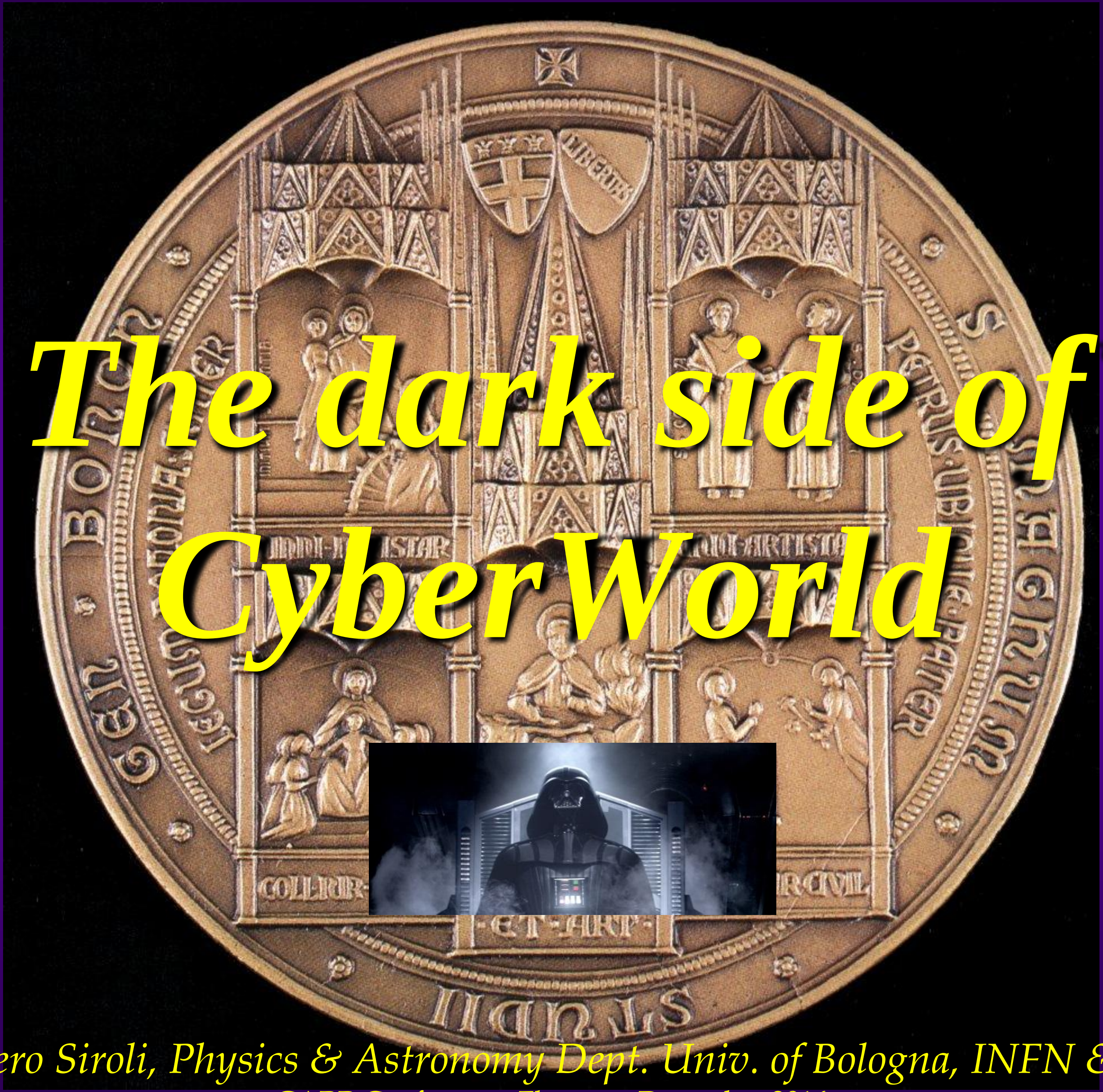
The dark side of CyberWorld



Gian Piero Siroli, Physics & Astronomy Dept. Univ. of Bologna, INFN & CERN

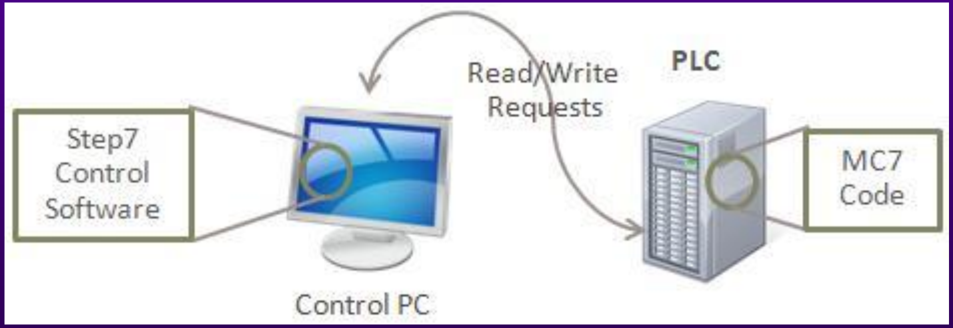
GARR Conference, Florence, December 2016

What a cyber-weapon can look like: Stuxnet

- A “worm” designed to sabotage a specific industrial process. It penetrates a particular subsystem of a SCADA industrial control systems of a single producer (Siemens). Once injected, it spreads silently in the Windows/SCADA infrastructure looking for specific Programmable Logic Controllers (PLC) and reprogram them to alter the functionality, showing at the same time normal running conditions to the monitoring system
- Reported in June 2010. First example of a precision military-grade cyber-weapon, deployed to seek and damage a real world physical target, operating the machinery outside its safe/usual performance envelope. Heavy insider knowledge, combination of cyber-war and intelligence
- Disruption of Iran's nuclear program by damaging centrifuges at uranium enrichment facility in Natanz
- Worm analyzed in public conferences, papers from various authors, probably the best studied piece of malware in history. Executable code available on the network

What is Stuxnet?

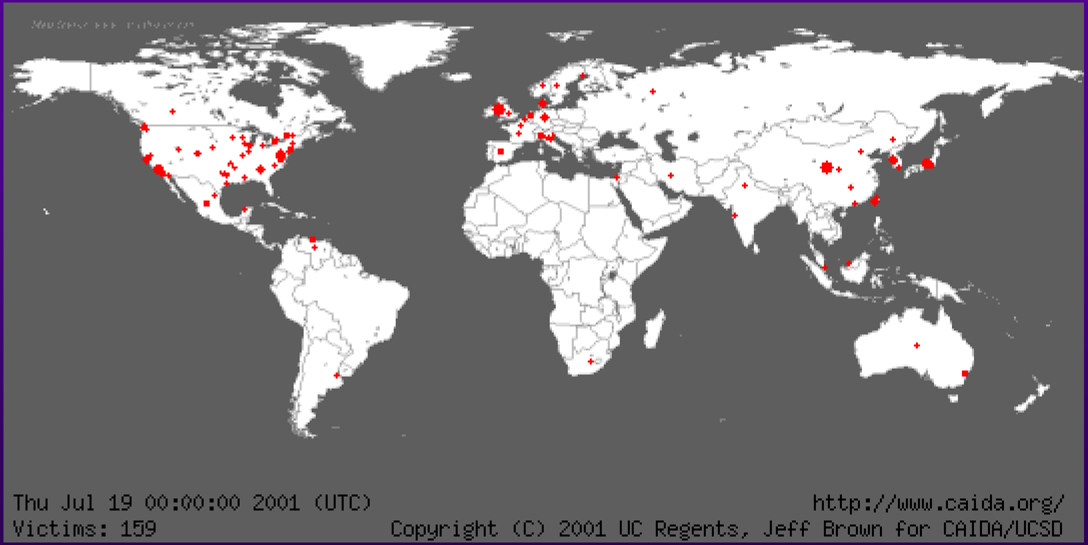
- How: Stuxnet intercepts communications with the PLC, determines whether the system is the intended target, modifies the existing PLC code to change the operational parameters. It hides the PLC infection from the operator using rootkit functionality. All these activities take place in two different environments: the Windows environment where the control software (WinCC/STEP7) is running AND at the PLC level, where the malicious code in assembly language (MC7) is injected and executed. Stuxnet determines the target asap and looks for specific configuration before activating



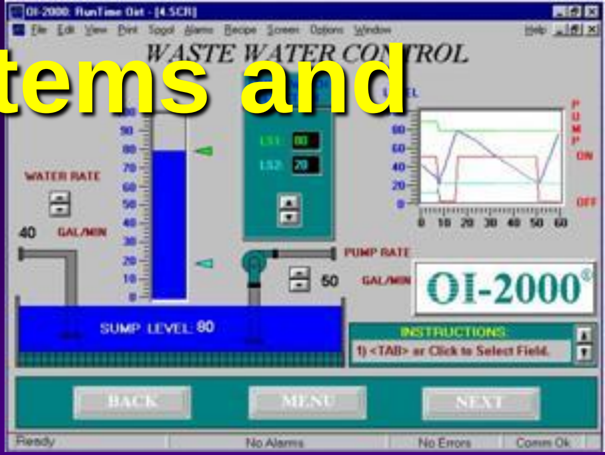
What is a worm

- Self-replicating segment of code able to autonomously spread travelling across networks without any human intervention. Usually containing a “payload” (malware) activating on target systems. A computer virus needs human activity (email, distribution of infected files) and an application to attach to

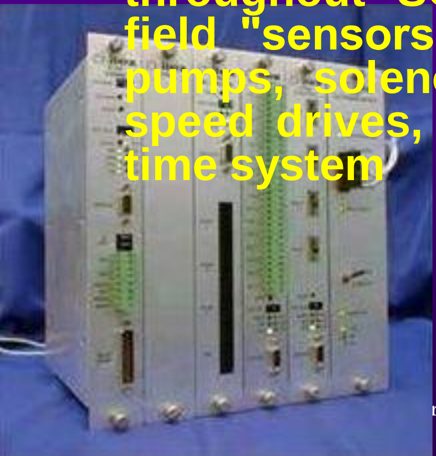
Code Red worm propagation during 24h following release (2001)


Thu Jul 19 00:00:00 2001 (UTC)
Victims: 159
http://www.caida.org/
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

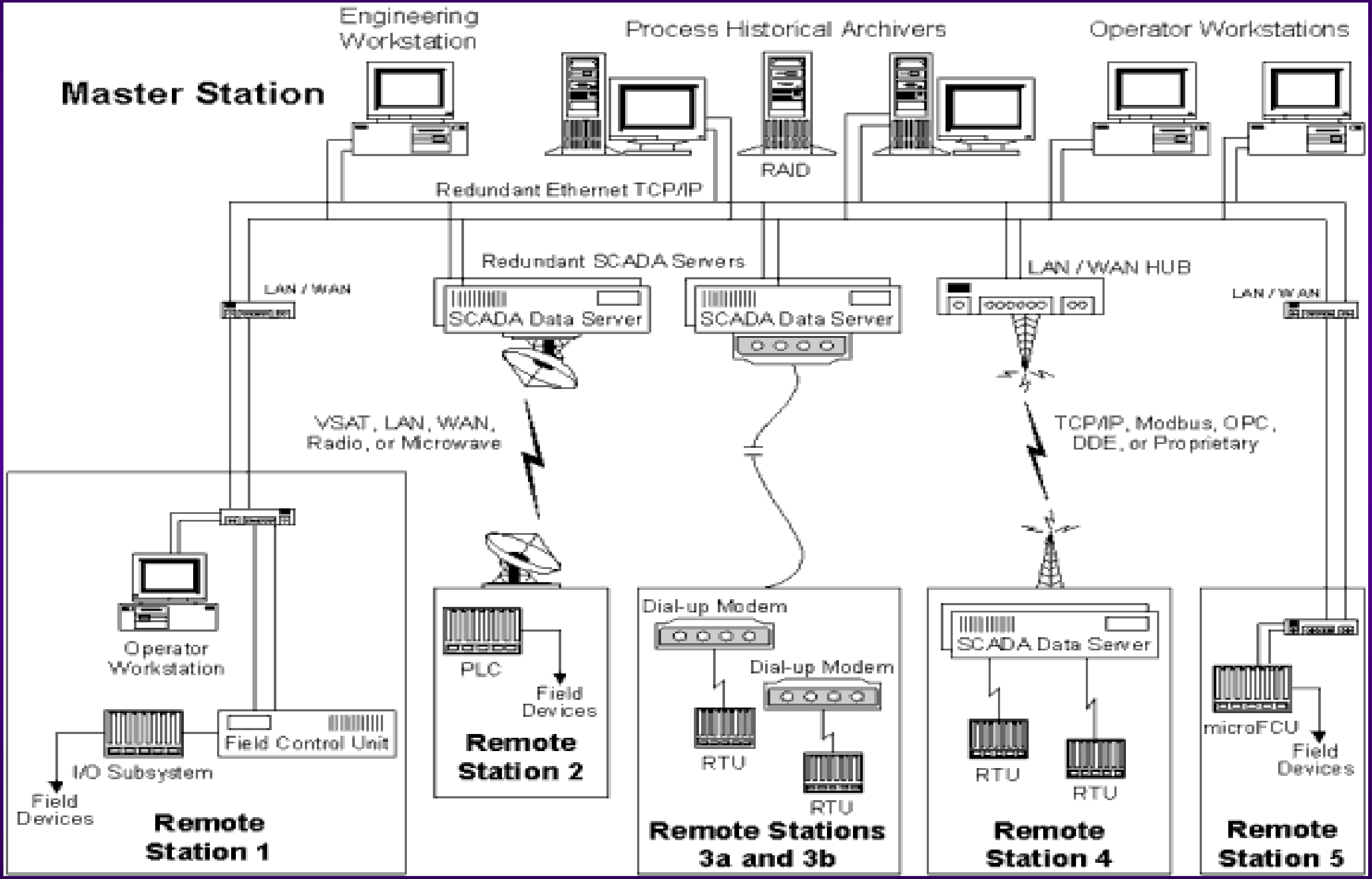
Industrial Control Systems and SCADA



- ICSs assist in the management of equipment found in critical infrastructure facilities (electric power generation & distribution, water and wastewater treatment, oil and gas refineries, chemical and food production, transportation). Acting on real daily life equipment
- SCADA (Supervisory Control and Data Acquisition) systems: highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation
- PLC (Programmable Logic Controllers): computer-based low level devices that control real world processes and equipment, used throughout SCADA (and DCS). Automation of field "sensors" and "actuators" (motor starters, pumps, solenoids, pilot lights/displays/devices, speed drives, valves, motion control). Hard real time system



Many intrusion vectors and open doors

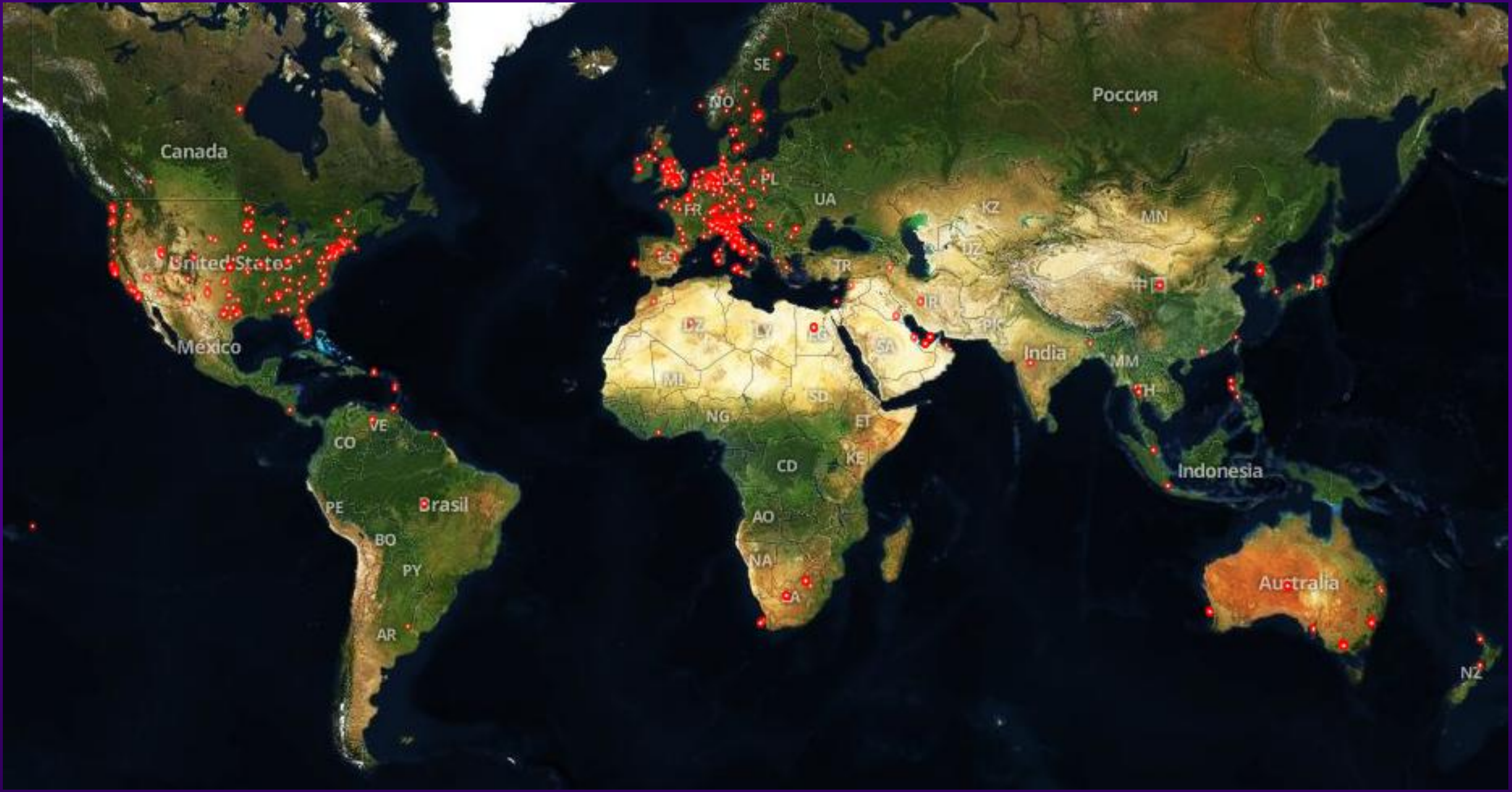


Critical infrastructures strongly dependent on ICT, intrinsically unsafe and vulnerable

- Security flaws inherent in Internet Protocol suite (TCP/IP, most widely used communication standard on the Internet). Security not was not a primary design consideration. Many attacks are “legal” actions according to protocols
- Faulty implementation of protocols and improper configuration
- Bugs in s/w code, flaws in architecture & design
- Security often not (properly) implemented
- Vulnerabilities of ICT underlying

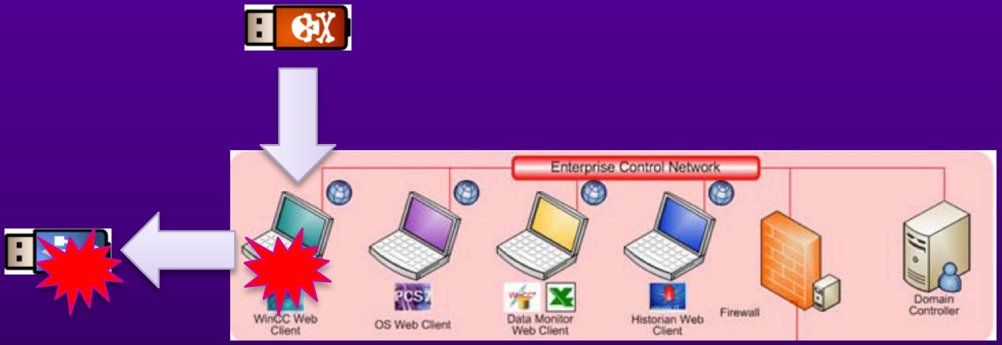
layer projected onto critical infrastructures

Vulnerabilities available on the net



First Infection: Enterprise Computer

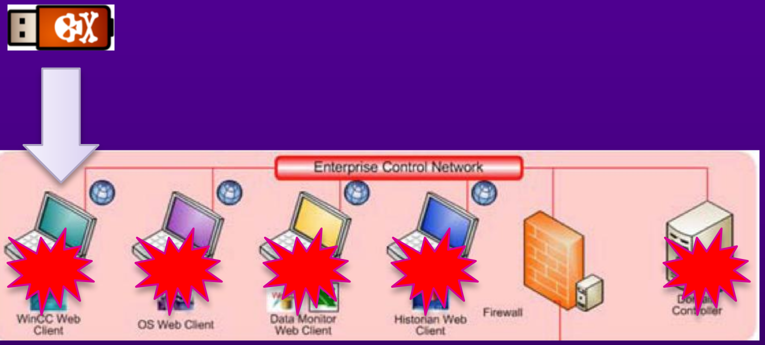
- Infected USB drive infiltrated into the plant and inserted into computer (employees laptop infected off-site, infected project files from contractor). Malicious act or through social engineering. “Air-gap” overcome
- Stuxnet successfully installs even though computer is fully patched and up to date with anti-virus signatures
- Rootkit installed to hide files and activities
- Attempts connection to Command-and-Control server for updates
- Infects any new USB Flash drive inserted into computer



(animation from E.Byres, Tofino Security)

Propagation on Enterprise Network

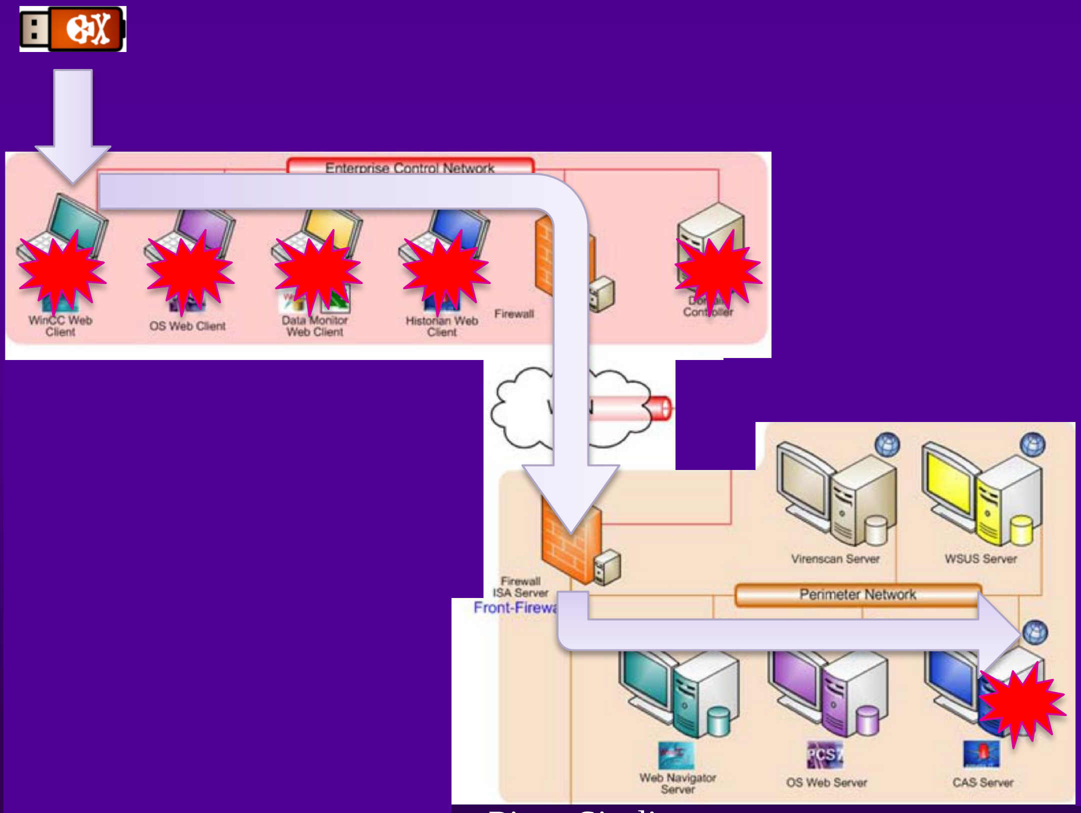
- Rapidly spreads to Print Servers and File Servers within hours of initial infection
- Establishes P2P network and access to C&C server (but the worm is autonomous, no remote control, “Launch and Forget”)
- Infects any new USB Flash drive inserted into any computer



(animation from E.Byres, Tofino Security)

Penetrating Perimeter Network

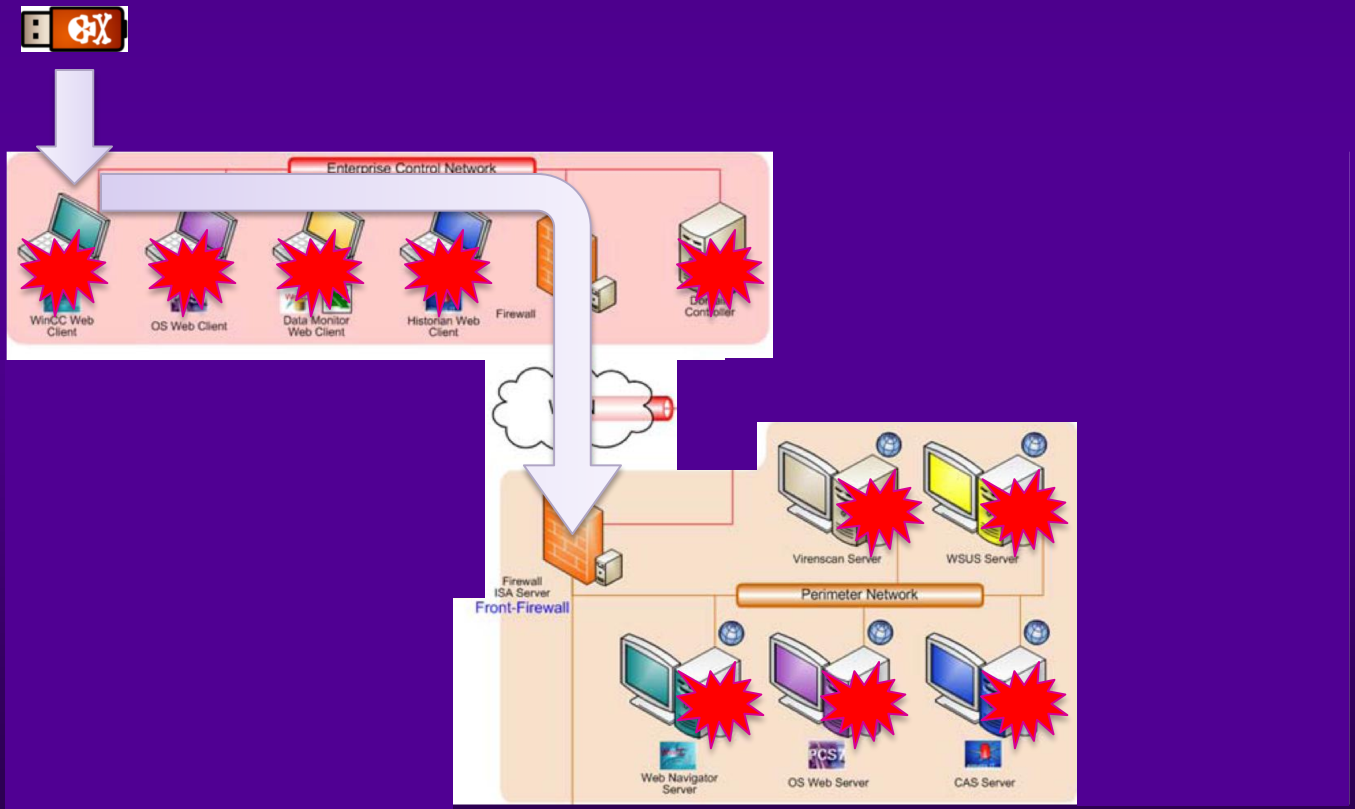
- **System Admin (Historian) becomes infected through network printer and file shares**
- **System Admin connects via VPN to Perimeter Network and infects the CAS Server and its WinCC SQL Server database**



(animation from E.Byres, Tofino Security)

Propagation on Perimeter Network

- Infects Web Navigation Server's WinCC SQL Server
- Infects STEP7 Project files
- Infects other Windows hosts on the subnet like WSUS, AVS etc

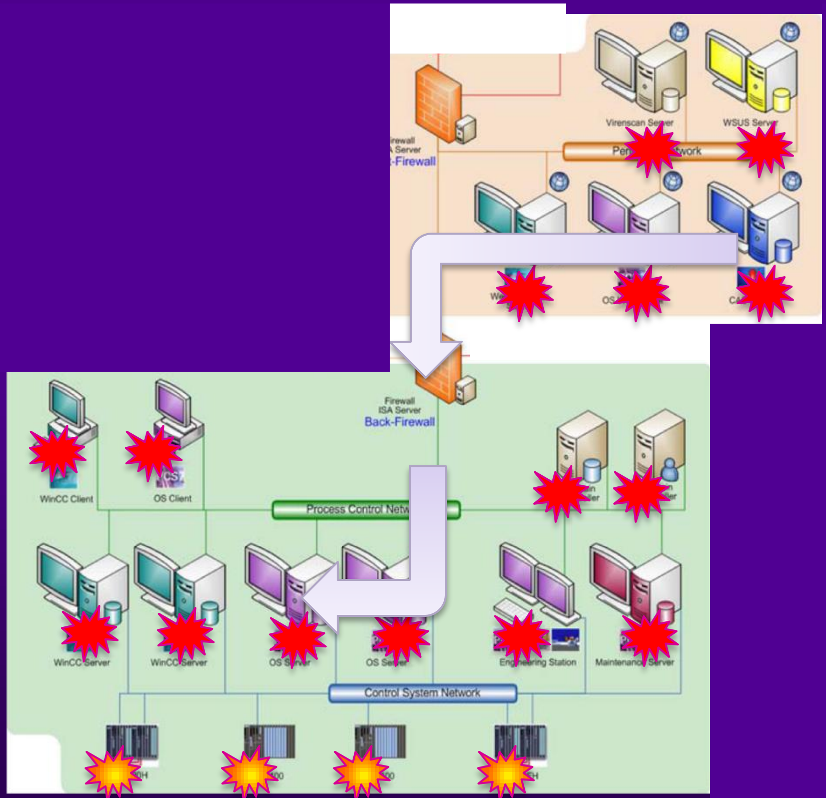


(animation from E.Byres, Tofino Security)

Propagation to Control Networks

- Leverages network connections between Perimeter and Process Control Network
- Exploits database connections between CAS Server (Perimeter) and Operator Station Server (PCN)
- Infects other hosts on PCN via Shares, WinCC or STEP7 methods

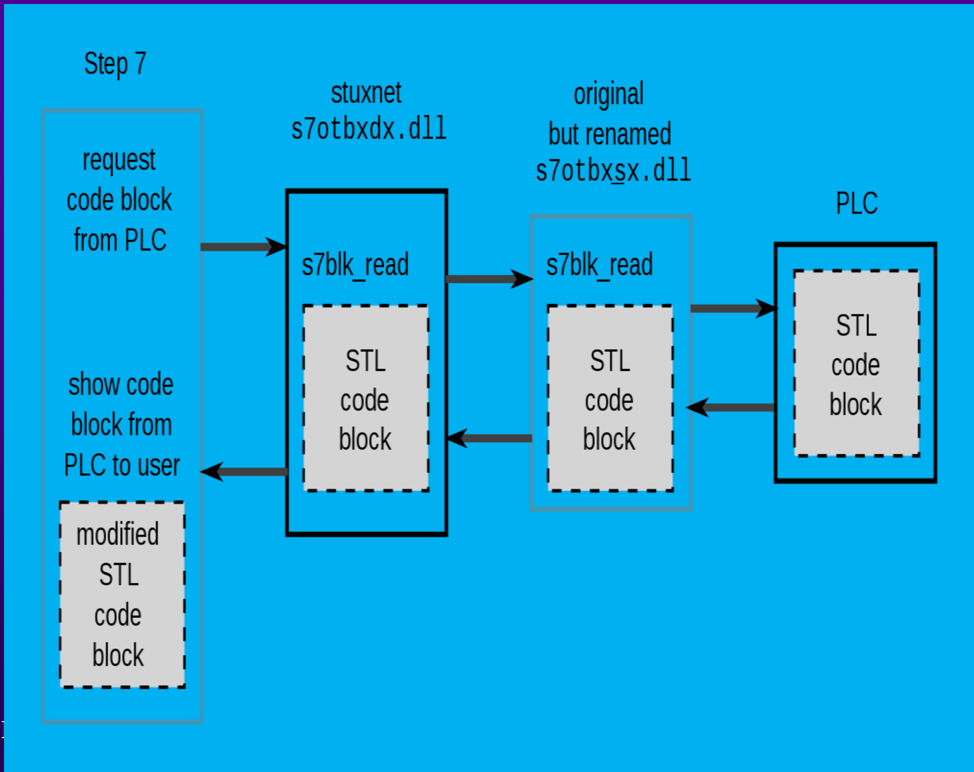
- …until it gets at the interface of the PLC level, and propagates further crossing it…



(animation from E.Byres, Tofino Security)

Final steps - I

- Stuxnet “fingerprints” the connected PLCs
- If the right PLC is found (only two Siemens CPUs are infected), it replaces the S7 communication libraries (DLLs) used for exchanging data with PLCs adding hidden functionality. Stuxnet is the vector to deliver the attack code (15000 LOC) to the PLCs
- Stuxnet is now controlling the communication between SCADA & PLC (“Man in the Middle”). It intercepts the input values from sensors and give fake (prerecorded) data to legitimate programs



Final steps - II

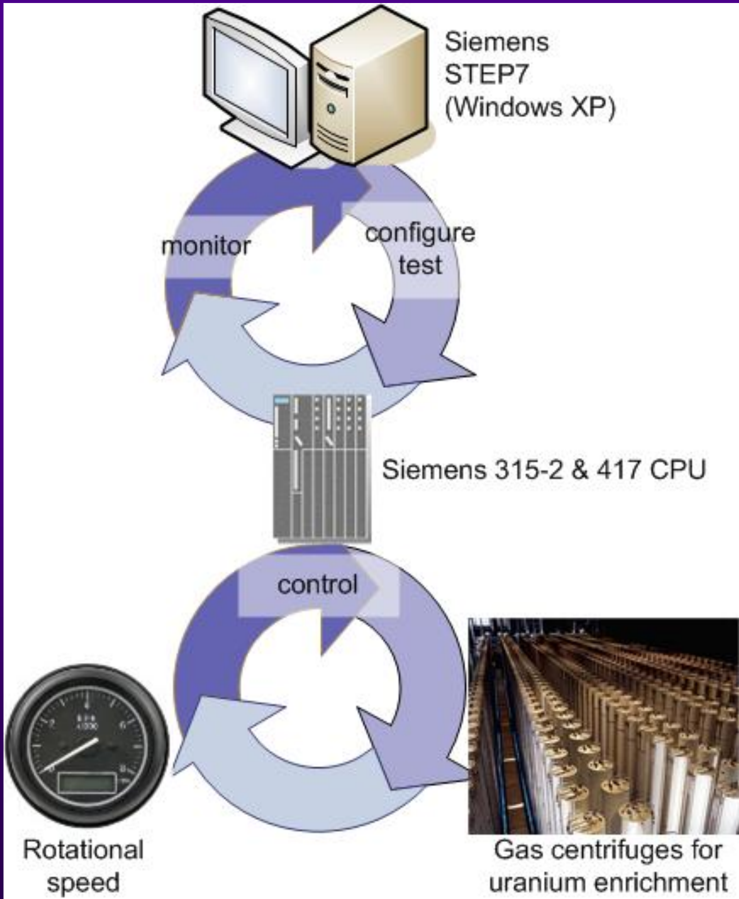
- Stuxnet downloads and replaces code and data to alter PLC behavior controlling the communication between PLC & control system. It intercepts the input values from sensors and give fake data to legitimate programs

This code varies the rotational speed of the centrifuges over months,

wearing them out by slowly cracking centrifuge rotors and inhibiting uranium enrichment

…in the meantime…

everything looks normal at the SCADA supervisor level

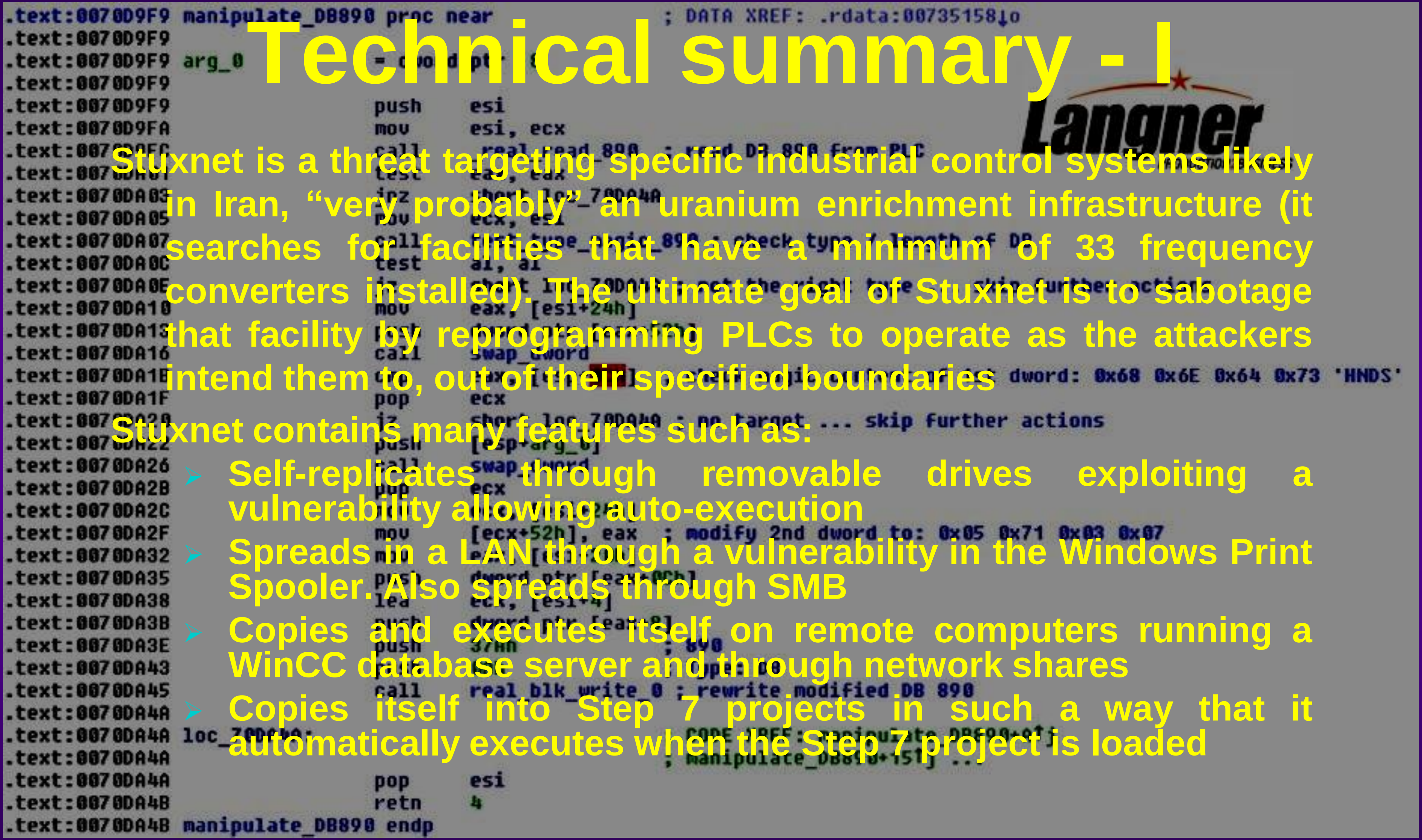


Technical summary - I

Stuxnet is a threat targeting specific industrial control systems likely in Iran, “very probably” an uranium enrichment infrastructure (it searches for facilities that have a minimum of 33 frequency converters installed). The ultimate goal of Stuxnet is to sabotage that facility by reprogramming PLCs to operate as the attackers intend them to, out of their specified boundaries

Stuxnet contains many features such as:

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution
- Spreads in a LAN through a vulnerability in the Windows Print Spooler. Also spreads through SMB
- Copies and executes itself on remote computers running a WinCC database server and through network shares
- Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded



```
.text:0070D9F9 manipulate_DB890 proc near          ; DATA XREF: .rdata:00735158↓o
.text:0070D9F9
.text:0070D9F9 arg_0           = dword ptr  8
.text:0070D9F9
.text:0070D9F9                 push    esi
.text:0070D9FA                 mov     esi, ecx
.text:0070D9FC                 call    real_read_890  ; read DB 890 from PLC
.text:0070DA01                 test    eax, eax
.text:0070DA03                 jnz     short loc_70DA4A
.text:0070DA05                 mov     ecx, esi
.text:0070DA07                 call    check_type_magic_890 ; check type, length of DB
.text:0070DA0C                 test    al, al
.text:0070DA0E                 jz      short loc_70DA4A ; not the right type, skip further actions
.text:0070DA10                 mov     eax, [esi+24h]
.text:0070DA13                 push    [illegible]
.text:0070DA16                 call    swap_dword
.text:0070DA1B                 [illegible]            ; [illegible] dword: 0x68 0x6E 0x64 0x73 'HNDS'
.text:0070DA1F                 pop     ecx
.text:0070DA20                 jz      short loc_70DA4A ; no target ... skip further actions
.text:0070DA22                 push    [esp+arg_0]
.text:0070DA26                 call    swap_dword
.text:0070DA2B                 pop     ecx
.text:0070DA2C                 [illegible]
.text:0070DA2F                 mov     [ecx+52h], eax  ; modify 2nd dword to: 0x05 0x71 0x03 0x07
.text:0070DA32                 [illegible]
.text:0070DA35                 push    dword ptr [eax+0Ch]
.text:0070DA38                 lea     ecx, [esi+4]
.text:0070DA3B                 push    dword ptr [eax+8]
.text:0070DA3E                 push    37Ah            ; 890
.text:0070DA43                 [illegible]
.text:0070DA45                 call    real_blk_write_0 ; rewrite modified DB 890
.text:0070DA4A
.text:0070DA4A loc_70DA4A:                             ; CODE XREF: manipulate_DB890+A↑j
.text:0070DA4A                                         ; manipulate_DB890+15↑j ...
.text:0070DA4A                 pop     esi
.text:0070DA4B                 retn    4
.text:0070DA4B manipulate_DB890 endp
```

Technical summary - II

- Updates itself through a P2P mechanism within a LAN, just injecting a new version of the worm
- Compromises the O/S by exploiting a total of four(!) zero-day exploits (unpatched MS vulnerabilities worth >$100k, two for self-replication and two for escalation of privilege) and it takes advantage of seven different propagation processes
- Establishes a P2P connection to a C&C server that allows the hacker to download and execute code, including updated versions. Autonomous cyber weapon system
- Contains a Windows rootkit that hides its binaries. Hides modified code on PLCs, first PLC rootkit ever seen
- Attempts to bypass security products. Signed with two trusted (stolen) digital certificates (for drivers) to avoid being detected
- Many different versions starting 6/2009
- Sophisticated techniques to limit/avoid reverse engineering of the code (encryption, anti-anti debug)
- One of the most complex and carefully engineered worms ever seen. Science-fiction code

Comments

- Stuxnet code is sophisticated, very large (about 0.5MB). Probably assembled by a large team of highly qualified experts in different fields with control system expertise, working during an extended period of time, with specific hardware equipment available for testing. The kind of resources needed to stage such an attack seems to point to a nation state. Early versions in/before 2009(?)
- Model for simple, destructive SCADA worms. It exploits inherent PLC design issues
- The attack involves heavy insider knowledge. Combination of cyber-war and intelligence
- Stuxnet, targeting a specific industrial control system, is responsible for the disruption of Iran's nuclear program by damaging centrifuges at uranium enrichment facility in Natanz (no other targets). Iranian President acknowledged the damage by the worm (distribution of infected hosts: 59% Iran, 18% Indonesia, 8% India)

ICS vulnerabilities:
back to this society…??

M.G.Coggiola

M.G.Coggiola

**…basic infrastructures,
almost ICT / ICS independent…**

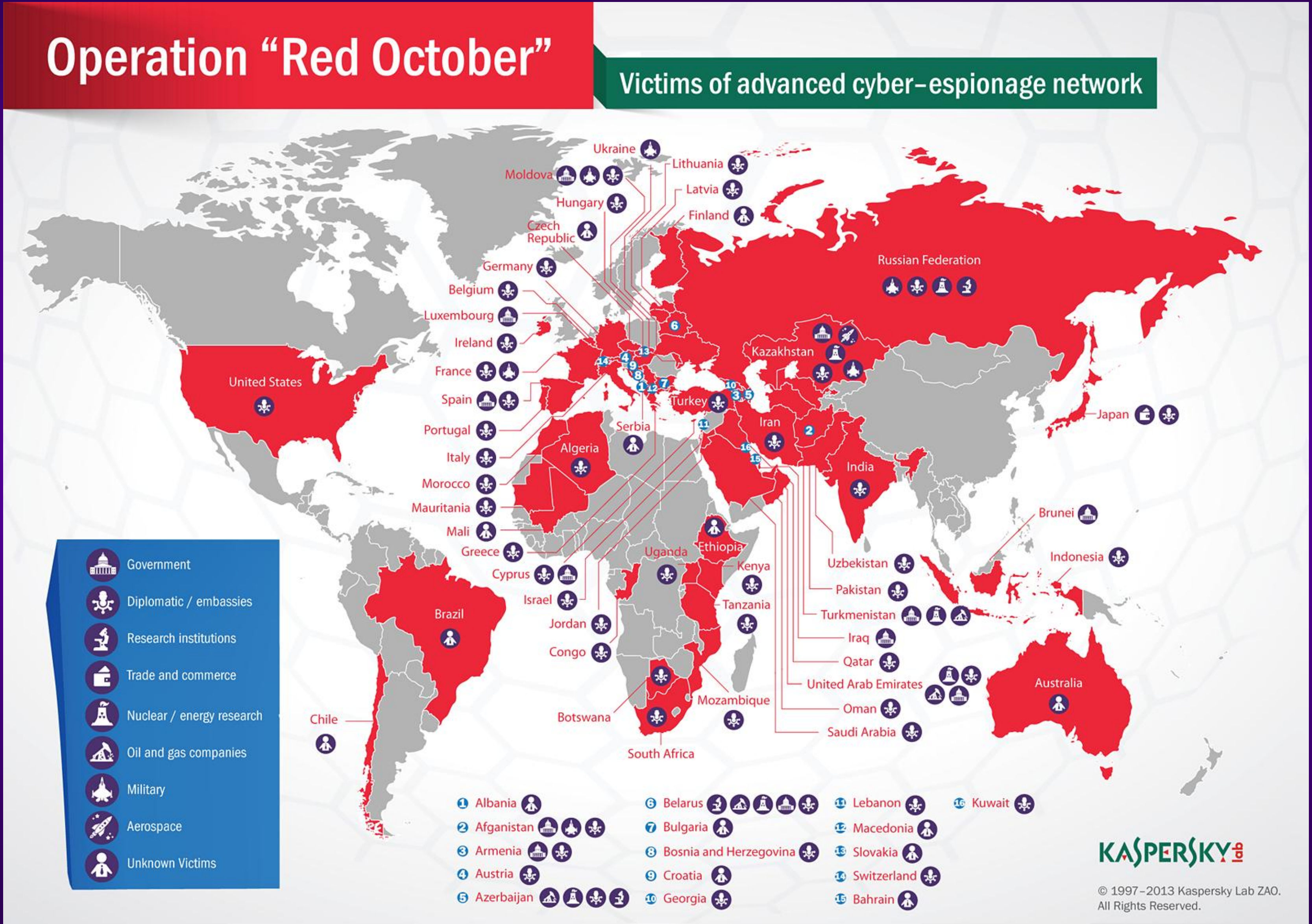
More cyberweapons

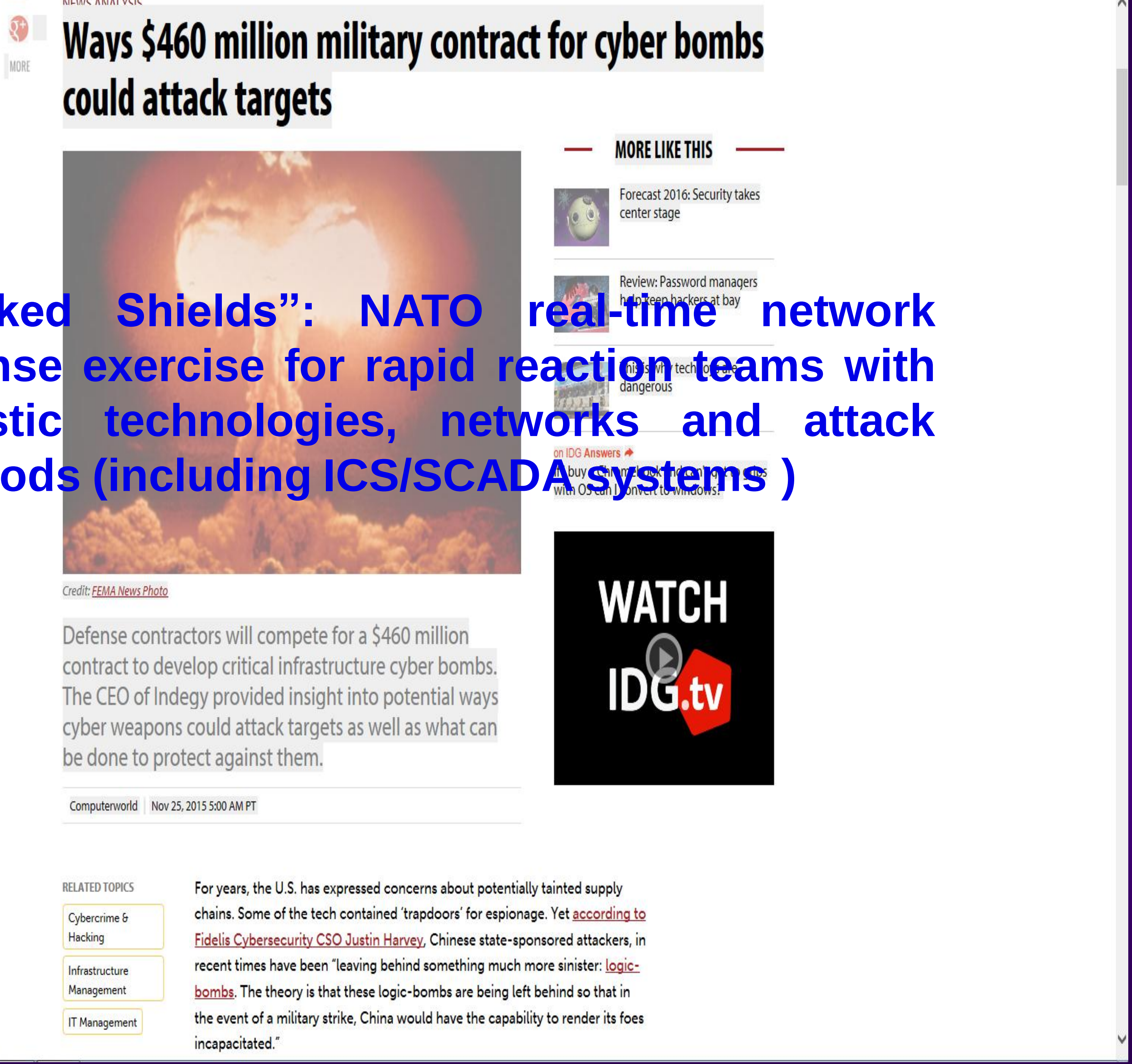
- Duqu (2011, Remote Access Trojan, not self-replicating, missing component?). Very similar to Stuxnet, targeting computers rather than ICS. Probably built for information gathering (back door, recording keystrokes and system information). Cyber-reconnaissance? Precursor of next Stuxnet-like attack?? Limited targets. Designed to last 36 days. Duqu2.0
- Flame (June 2012 reported in Iran). Optimized for espionage, at least two years old, mainly confined in Iran and Middle East. Large and complex, impressive espionage capabilities: recording voice and skype conversations, screenshots, keyboard activity, network traffic. No automatic replication/propagation (stealthier and better targeting). "Self destruct" module to eliminate traces and avoid code analysis. Connection to Stuxnet, commissioned by the same nations?
- Gauss (summer 2012) - Nation-state sponsored banking Trojan for info stealing, monitor bank accounts & financial circuits flow. Similarities with Flame. Distributed mainly in Lebanon, Israel, Palestine. Mysterious encrypted payload surgically targeted. Developed by Flame/Stuxnet creators??
- Shamoon (summer 2012) - cyber-sabotage in oil & energy sectors (Saudi company Aramco). Similarities with Flame
- Red October (January 2013) - advanced cyber espionage network targeting diplomatic/governmental agencies and scientific research organizations attacking computers, mobile phones, network equipment

…and more to come…

the next one might already be on your desktop, laptop, smartphone

Red October


Operation “Red October”
Victims of advanced cyber–espionage network
Government
Diplomatic / embassies
Research institutions
Trade and commerce
Nuclear / energy research
Oil and gas companies
Military
Aerospace
Unknown Victims
Ukraine
Moldova
Hungary
Czech Republic
Germany
Belgium
Luxembourg
Ireland
France
Spain
Portugal
Italy
Morocco
Mauritania
Mali
Greece
Cyprus
Israel
Jordan
Congo
Lithuania
Latvia
Finland
Russian Federation
Kazakhstan
Turkey
Serbia
Iran
Algeria
United States
Japan
India
Brunei
Indonesia
Ethiopia
Uganda
Kenya
Tanzania
Brazil
Chile
Botswana
Mozambique
South Africa
Australia
Uzbekistan
Pakistan
Turkmenistan
Iraq
Qatar
United Arab Emirates
Oman
Saudi Arabia
1 Albania
2 Afganistan
3 Armenia
4 Austria
5 Azerbaijan
6 Belarus
7 Bulgaria
8 Bosnia and Herzegovina
9 Croatia
10 Georgia
11 Lebanon
12 Macedonia
13 Slovakia
14 Switzerland
15 Bahrain
16 Kuwait
KASPERSKY lab
© 1997–2013 Kaspersky Lab ZAO.
All Rights Reserved.



Ways $460 million military contract for cyber bombs could attack targets

MORE LIKE THIS

Forecast 2016: Security takes center stage

Review: Password managers help keep hackers at bay

This is why tech toys are dangerous

on IDG Answers

If I buy Chromebook and can't get to grips with OS can I convert to windows?

Credit: FEMA News Photo

Defense contractors will compete for a $460 million contract to develop critical infrastructure cyber bombs. The CEO of Indegy provided insight into potential ways cyber weapons could attack targets as well as what can be done to protect against them.

Computerworld | Nov 25, 2015 5:00 AM PT

RELATED TOPICS

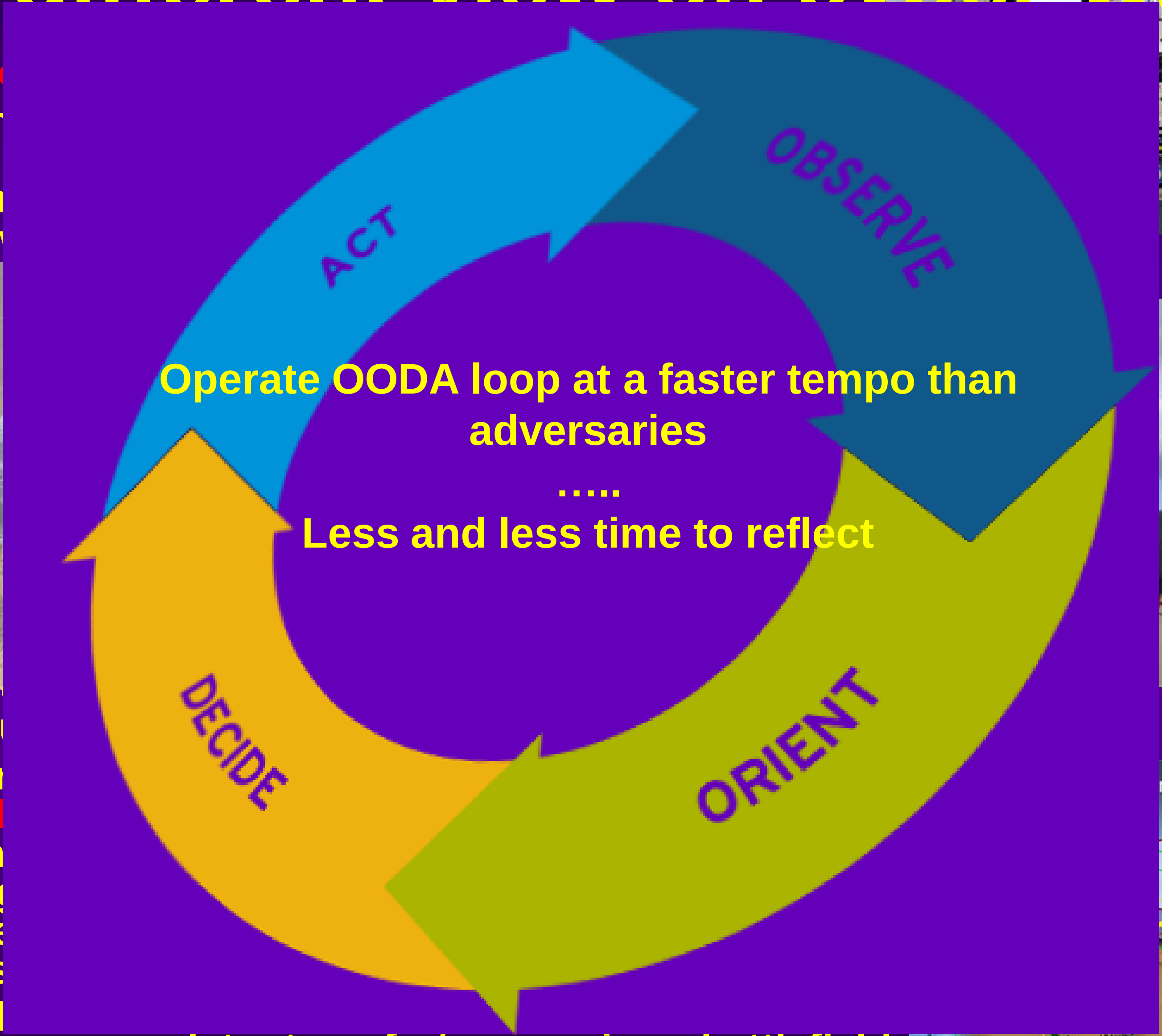
- Cybercrime & Hacking
- Infrastructure Management
- IT Management

For years, the U.S. has expressed concerns about potentially tainted supply chains. Some of the tech contained 'trapdoors' for espionage. Yet according to Fidelis Cybersecurity CSO Justin Harvey, Chinese state-sponsored attackers, in recent times have been "leaving behind something much more sinister: logic-bombs. The theory is that these logic-bombs are being left behind so that in the event of a military strike, China would have the capability to render its foes incapacitated."

"Locked Shields": NATO real-time network defense exercise for rapid reaction teams with realistic technologies, networks and attack methods (including ICS/SCADA systems)

A different view on cyber-war

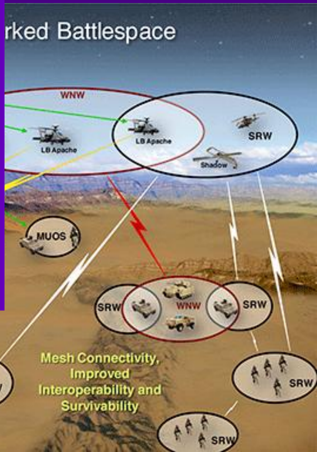
- Threat t
  - Vuln s/w com netw equ
  - Cyb disru
  - Dron
- Battlefield d
  - Airborn technolog exchange awarenes
  - High sp voice & sensor data transfer/processing, battlefield surveillance, C&C. Mobile “ad-hoc” & sensor networks

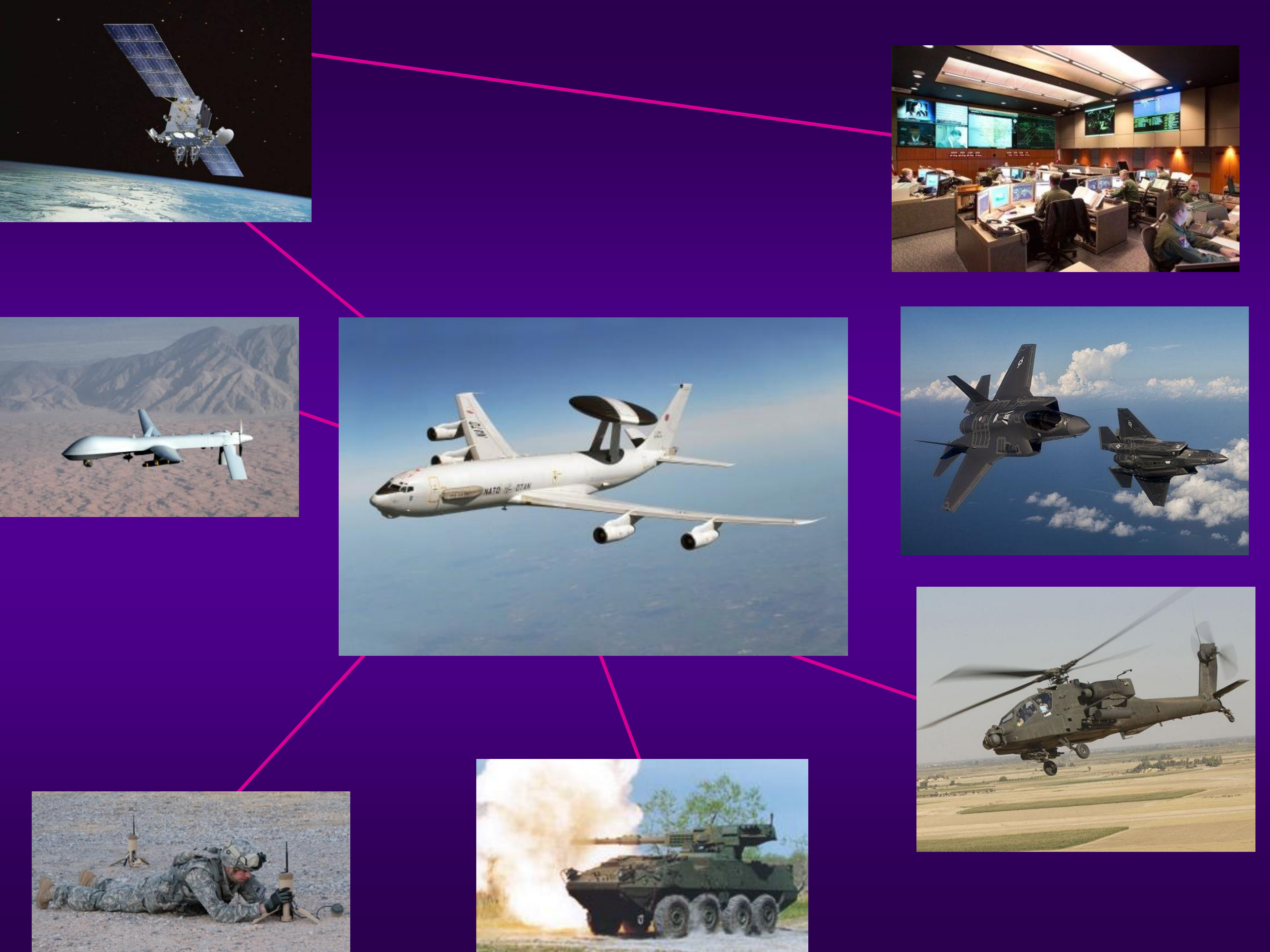


Operate OODA loop at a faster tempo than adversaries

…..

Less and less time to reflect

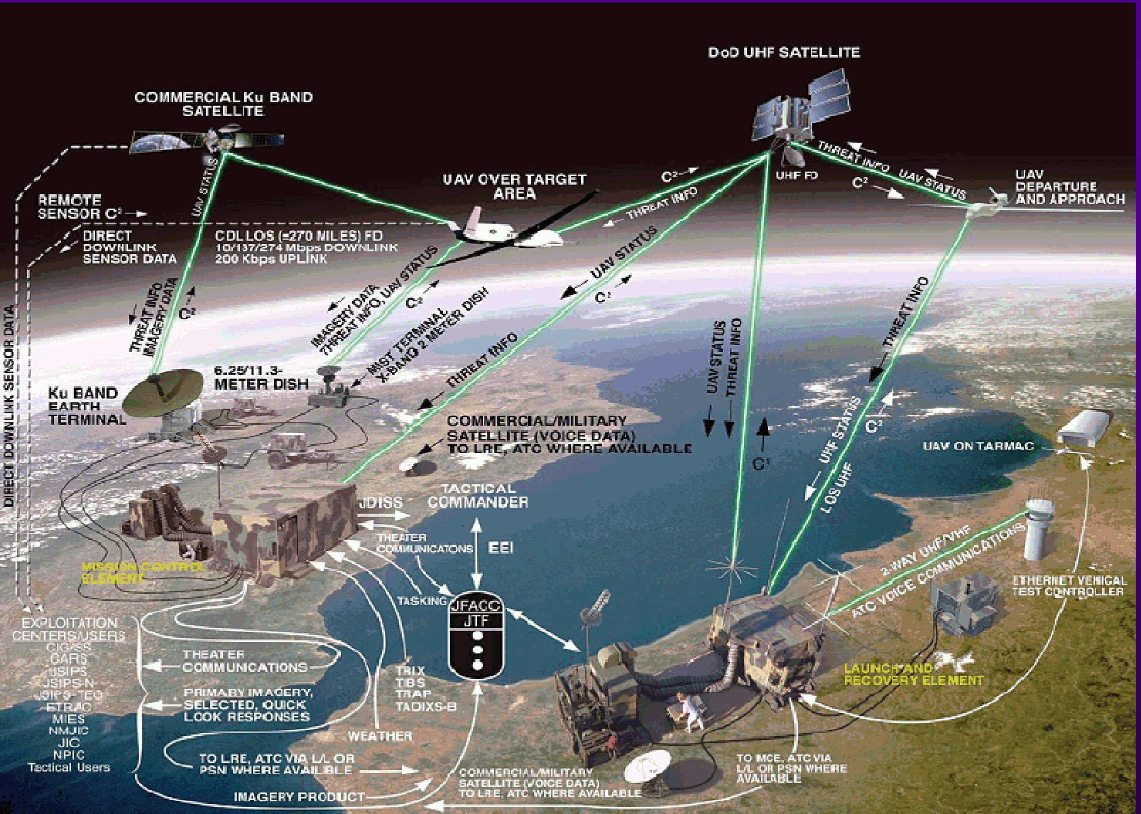

rked Battlespace
WNW
LB Apache
SRW
Shadow
MUOS
Mesh Connectivity, Improved Interoperability and Survivability


NATO OTAN

F-35 cockpit

Global Hawk UAV

- Continuous day/night, high altitude, long endurance, all weather surveillance & reconnaissance in direct support of ground and air forces, sensor data to tactical units. Strike. Visual, IR, SAR imagery. Intelligence gathering, terrain obs, targeting. (UGV, UUV)
- Integrated system: mission control (plan, C&C, communications, monitoring), launch/recovery, vehicle tests


DoD UHF SATELLITE
COMMERCIAL Ku BAND SATELLITE
UAV OVER TARGET AREA
REMOTE SENSOR C²
DIRECT DOWNLINK SENSOR DATA
CDL LOS (≈270 MILES) FD
10/137/274 Mbps DOWNLINK
200 Kbps UPLINK
UAV STATUS
THREAT INFO
IMAGERY DATA
C²
IMAGERY DATA, THREAT INFO, UAV STATUS
MIST TERMINAL X-BAND 2 METER DISH
THREAT INFO
UHF FD
UAV DEPARTURE AND APPROACH
UAV STATUS
THREAT INFO
C¹
UHF STATUS
LOS UHF
Ku BAND EARTH TERMINAL
6.25/11.3-METER DISH
COMMERCIAL/MILITARY SATELLITE (VOICE DATA) TO LRE, ATC WHERE AVAILABLE
UAV ON TARMAC
DIRECT DOWNLINK SENSOR DATA
JDISS
TACTICAL COMMANDER
THEATER COMMUNICATONS
EEI
MISSION CONTROL ELEMENT
2-WAY UHF/VHF ATC VOICE COMMUNICATIONS
ETHERNET VEHICAL TEST CONTROLLER
TASKING
JFACC
JTF
EXPLOITATION CENTERS/USERS
CIGSS
CARS
JSIPS
JSIPS-N
JSIPS-TEG
ETRAC
MIES
NMJIC
JIC
NPIC
Tactical Users
THEATER COMMUNICATIONS
PRIMARY IMAGERY, SELECTED, QUICK LOOK RESPONSES
TRIX
TBS
TRAP
TADIXS-B
LAUNCH AND RECOVERY ELEMENT
WEATHER
TO LRE, ATC VIA L/L OR PSN WHERE AVAILABLE
IMAGERY PRODUCT
COMMERCIAL/MILITARY SATELLITE (VOICE DATA) TO LRE, ATC WHERE AVAILABLE
TO MCE, ATC VIA L/L OR PSN WHERE AVAILABLE

- Hardware attacks during maintenance/storage: corrupt data stored on board, install extra components
- Remote cyber attacks during ops through comms: alter data on board (vehicle/system state, navigational, C2), break encryption of comm channel
- Sensor spoofing: GPS spoofing, blind vision sensors
- Buffer ovfl through some input device, event triggering, forced sys.reset, malicious code & packets, overload & DoS CPU/controllers…
- Dependence on uninterrupted comms: failures/accidents due to environmental EMI, EW threats, jamming

US RQ-170 Sentinel UAV incident

On 4 Dec 4th 2011 lost control of a CIA operated UAV while flying along Afghanistan-Iran border, downed and captured

GPS jamming & spoofing? Support by Russia?
Accidental crash landing?

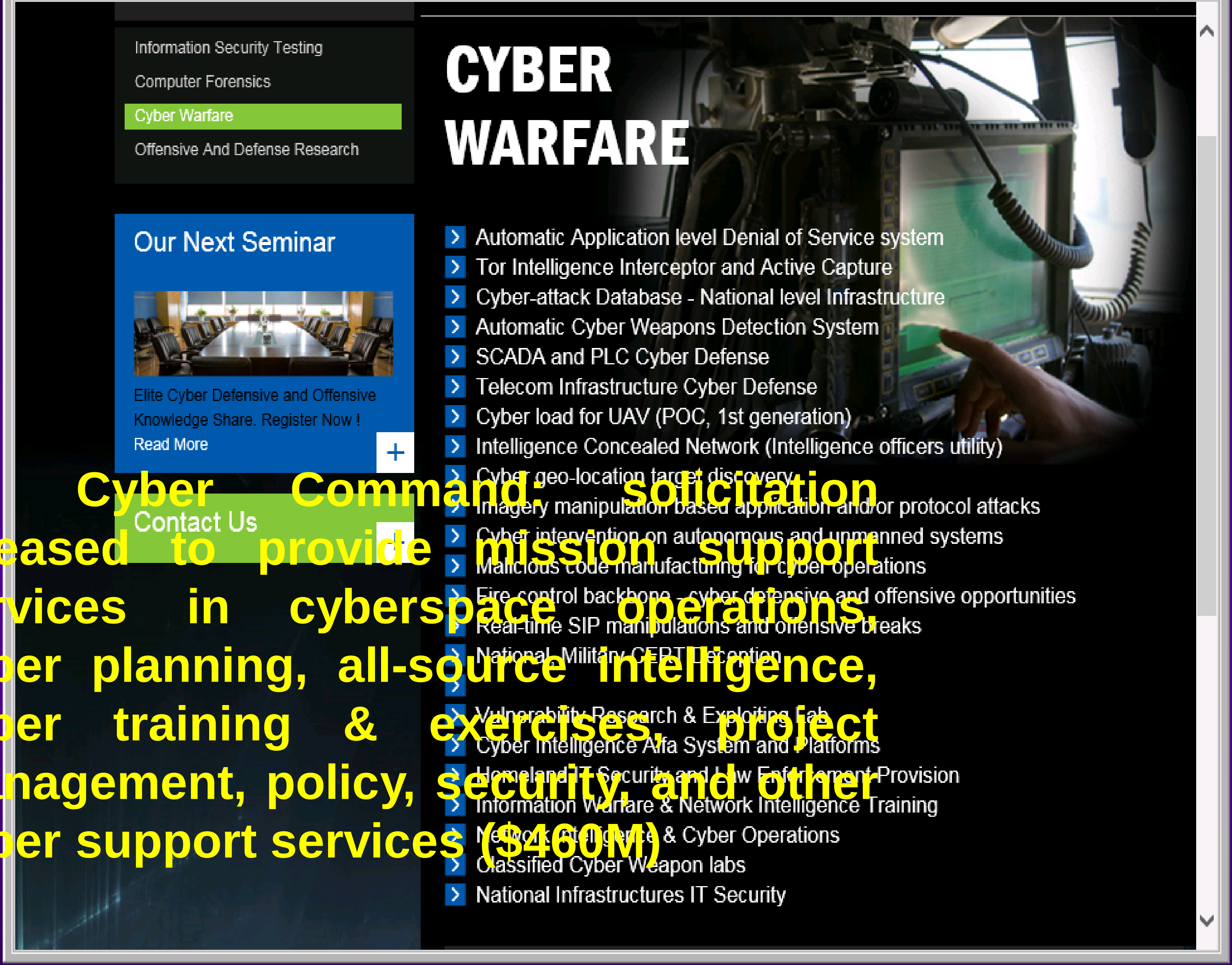
Stealth sophisticated drone, very significant loss

Iran has hunted/recovered two more UAV types since 2011: two RQ-11s and at least one ScanEagle

Oct 2016: Iran unveils new UCAV modeled(?) on captured US RQ-170

RTR8GE secure battlefield router for mission-critical communications and information sharing
(GE & Juniper Networks)

Insatiable demand for bandwidth and onboard processing capability in UAV platforms



Information Security Testing

Computer Forensics

Cyber Warfare

Offensive And Defense Research

Our Next Seminar

Elite Cyber Defensive and Offensive Knowledge Share. Register Now !

Read More +

Contact Us

CYBER WARFARE

- Automatic Application level Denial of Service system
- Tor Intelligence Interceptor and Active Capture
- Cyber-attack Database - National level Infrastructure
- Automatic Cyber Weapons Detection System
- SCADA and PLC Cyber Defense
- Telecom Infrastructure Cyber Defense
- Cyber load for UAV (POC, 1st generation)
- Intelligence Concealed Network (Intelligence officers utility)
- Cyber geo-location target discovery
- Imagery manipulation based application and/or protocol attacks
- Cyber intervention on autonomous and unmanned systems
- Malicious code manufacturing for cyber operations
- Fire control backbone - cyber defensive and offensive opportunities
- Real-time SIP manipulations and offensive breaks
- National Military CERT Deception
- Vulnerability Research & Exploiting Lab
- Cyber Intelligence Alfa System and Platforms
- Homeland IT Security and Law Enforcement Provision
- Information Warfare & Network Intelligence Training
- Network Intelligence & Cyber Operations
- Classified Cyber Weapon labs
- National Infrastructures IT Security

US Cyber Command: solicitation released to provide mission support services in cyberspace operations, cyber planning, all-source intelligence, cyber training & exercises, project management, policy, security, and other cyber support services ($460M)

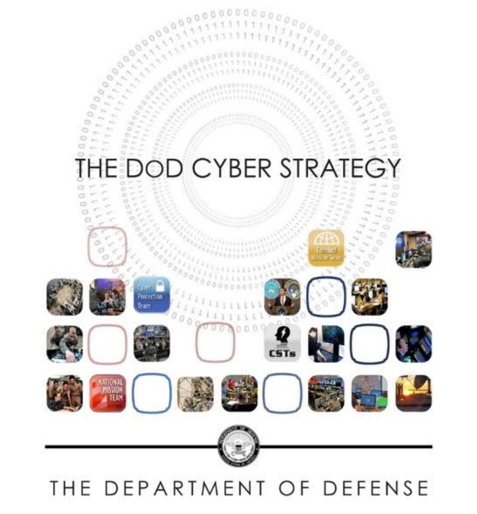
Cyber-warfare "products"

¿ Cyber-war ?

- ’80s - Siberia: pipeline explosion
- ~2000 - Serbia: ICT attack on air defense system. Iraq: attack on banking and telephony networks
- 2005 - Greece: ICT intrusion in mobile communication system by foreign intelligence
- USA: various electrical blackouts on a regional scale by cyber attacks
- 2007 - Estonia: prolonged attack against many national organizations (finance, public administration, media)
- 2008 - Syria, Georgia: cyber attack targeting air defense system and C&C centres in support of conventional operations
- 2009 - USA: video feeds of drones (Iraq) intercepted
- 2010 - USA: unified Cyber Command (CYBERCOM)

STUXNET

US DoD cyber strategy



THE DOD CYBER STRATEGY

THE DEPARTMENT OF DEFENSE

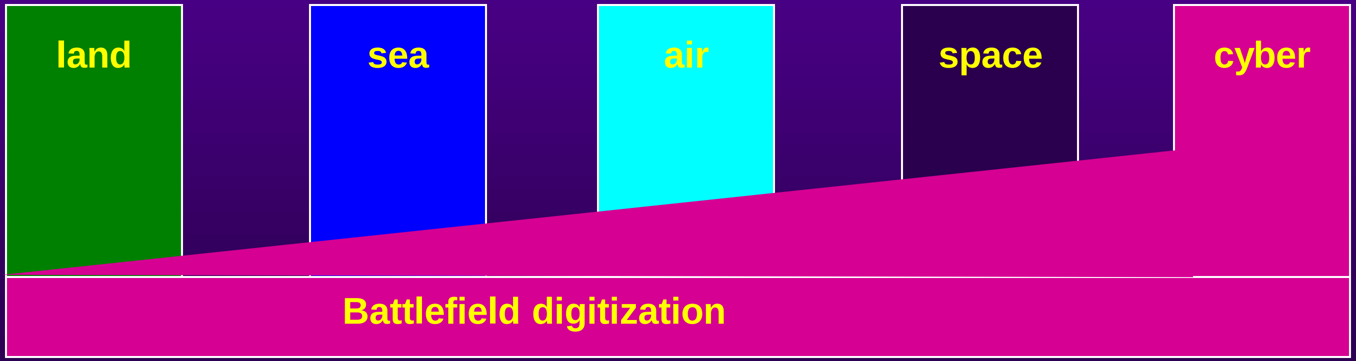
- **Primary missions:**
  - **Defend DoD networks, systems, information**
  - **Defend the US homeland & national interests against cyberattacks of significant consequence**
  - **Provide cyber support to military operational and contingency plans**

- **Building bridges to the private sector and beyond. Attract best talent, ideas, technology**
- **Deterrence key part of cyber strategy**
- **Build & maintain ready forces & capabilities to conduct cyber ops & control conflict escalation**
- **Build international partnership to deter threats and increase security & stability**

Comments on cyber-war

- Most dangerous parts of Stuxnet are generic, not specific to uranium enrichment plants, can be copied and modified to work in different environments. Delivery in different ways than USB sticks (remember Code Red). Discovered executables using (parts of) Stuxnet source code
- Cyber is a “once-only” weapon (lost after delivery)? Cyber-weapons proliferation?
- Many countries have technology and skills to initiate cyber attacks. Cyberspace already militarized, digital arms race?
- Cyber-war <- Battlefield digitization <- Electronic Warfare

ICT & microelectronics (r)evolution in warfare techniques and battlefield (sensors, computers, telecommunications, data processing systems). ICT (dual use technology) inter-domain underlying layer (cyber->anywhere)



Comments on cyber-war

- Cyber is an autonomous operational warfare domain. Cyber-only-war will probably never exist
- Is “cyber” different from land, sea, air, and space warfare operative domains? Artificial dimension created by man. Cyber-space is both a weapon AND a target at the same time?! Space/topology of the weaponry can be affected by the weapon (like if weapons used in warships could change the geography of oceans). Cyber-topology VERY volatile: regions of cyberspace appear/disappear on command or under (cyber/conventional) attack. Different “geography” from different locations
- Asymmetric war: dependency on vulnerable complex infrastructures. Asymmetry of actors, costs and vulnerabilities. Technological dependence on h/w (f/w) & s/w producers
- Wide and inter-disciplinary domain (technical, socio-political). Need to develop a new global vision/vocabulary
- Conflict & pre-conflict activities (PSYOPS)

Specific features of cyber-warfare
(mixing of strategic, operational and tactical levels)

- Mobility of cyber-weapons (worms), propagation speed of ops very high. Maneuverability
- Striking power, fire capacity: volume, range, speed at which cyber-operations can be conducted. Definitions? Comparison with conventional domains?
- Network interconnections/integration, (near) real-time system (ability to successfully engage time-sensitive targets anywhere in the world). Sensor to shooter: integration with battlefield sensors systems/platforms
- Very high level of automation. Automation of C&C (decreased time from identification to engagement). Cyber RoE (man-out-of-the-loop)? No need to enable cyber-weapon, just release it on the net. Autonomous target search/guidance (or logic conditions to trigger payload), “Fire and Forget”

Specific features of cyber-warfare

- Fast global communications (situational awareness). Large amount of data (battlefield digitization)
- Defense/protection (of weapons and network/territory)? Attack?
- Territorial (i.e. network) characteristics: territorial penetration/destruction. Territorial control/denial?? Is network/territory valuable? Geography (network topology) under human control and vulnerable, very mutable environment, dynamically created and destroyed. Limits? Vulnerability/domination of chokepoints (rapidly changing). Operations in hostile environment
- Offense dominance!? Offense (destabilizing, first/preemptive strike) VS defense (stabilizing) balance. Cyber precursor of conventional attacks? High cost of defense, effectiveness?

Specific features of cyber-warfare
(strategic level)

- Deterrence (nuclear age concept) applicable to a cyber-weapon system?? Deterrence by retaliation complicated by attribution problem (difficult direct identification of attacker, at geopolitical level?!). MAD at cyber level?!
- When a cyber-attack can be considered an "act of war"? Limits in peacetime? Right to respond with traditional kinetic options: "The US reserves the right…to respond to serious cyber attacks with an appropriate proportional and justified military response". Definition of cyber-attack?
- Changeability
  - Technological: very rapid deployment of new technologies (time-to-battlefield). Fast technological development can change the nature of cyber-power?
  - Human: expertise increase slowly over time

Specific features of cyber-warfare

(strategic level)

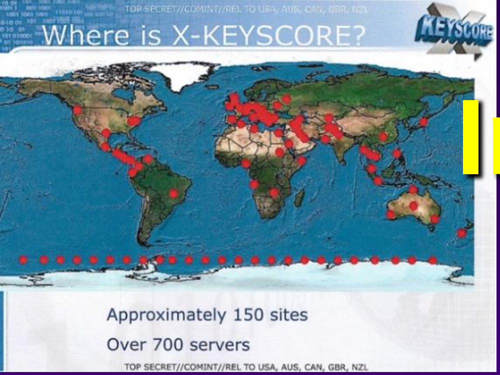
- New source of intelligence
- Is verification possible (agreements/treaties) in cyber-domain? Detection difficult. Cyber-weapons control??
- “Cyber” best for? Guerrilla-like operations? Intelligence, sabotage, single time-limited/highly targeted attacks? Support to conventional operations? Short or long term advantages? Consequences on other warfare domains (digitization, structures)?
- Integration/predominance of X-warfare (land, air, sea, space, cyber)? Is global stability increased or decreased by adding one more dimension?
- Man “in”, “on”, “off” the loop

Information Warfare e PSYOP

- Internet as a global communication “medium”
- Information Operations (IO): info manipulation for (counter)propaganda, disinformation, consensus building, discrimination, defamation, delegitimation, doxing, censorship/content filtering. Deception, perception war, influence ops manipulating target's values, beliefs, emotions, motives, reasoning, behavior. Traditional techniques on a new medium. Counterintelligence, ops security

“Nihil est quod videtur” “..Cicero..”

- Real world examples: support to dissident groups, recruitment campaigns, use/manipulation of social media/networks. Wikileaks (2010, Assange), NSAleaks (2013, Snowden), EZLN (‘90)
- Network is an ubiquitous surveillance environment
- Info war: primary political (strategic) value. “cyber influence” might contribute to political and social instability of a country. Blurring distinction between military and civilian domains


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?

Approximately 150 sites

Over 700 servers

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Inside NSA TAO hacking unit

Rob Joyce, head of NSA's Tailored Access Operations:
“A lot of people think that nation states are running their operations on zero days, but it's not that common. For big corporate networks, persistence and focus will get you in without a zero day; there are so many more vectors that are easier, less risky, and more productive”

Credential stealing as attack vector

infected devic

- **“Xkeyscore”: … et. >700 servers at ~150 sites wh… ing and analyzing global Internet**
- **“Angry Neighb… ch”: implants of a large number**
- **“Quantum”: s… orm attacks in a largely autom… inkedIn, Youtube, Twitter, Hotma… he market!?!**

GCHQ surveillance and propaganda

- Set of exploit tools from JTRIG (Joint Threat Research Intelligence Group), a unit of the British GCHQ
- UK MoD secret, multimillion-pound research program into the future of cyber-warfare, including how emerging technologies such as social media and psychological techniques can be harnessed by the military to influence people's mind and beliefs
- “Miniature Hero”: Active Skype capability. Provision of real time call records and bidirectional instant messaging
- “Hacienda”: scans open ports on all public servers to seek out vulnerabilities (~30 different countries scanned). ORBs
- “Scrapheap Challenge”: perfect spoofing of emails from Blackberry targets. “Underpass”: Change outcome of online polls. ”Gestator”: amplification of a given message, normally video, on popular multimedia websites (YouTube)

What about privacy & human rights??

Unit 8200

- According to intelligence analysts, IDF Unit 8200’s role similar to NSA or GCHQ, covering everything from SIGINT, code deciphering, use of human operators, open source information analysis
- Special unit devoted to cyber-war
- Involved in STUXNET? Flame? (UPI)
- Mutual exchange of raw signals intelligence between Israeli SIGINT National Unit and US NSA? (E.Snowden)
- Unit 8200 incubator: Israel's high-tech companies "flooded" with Unit alumni. Check Point, Nice, Comverse, CyberReason, ICQ, Palo Alto Networks, Onavo all directly influenced by 8200 technology
- Private Israeli Company Collects Counter-terrorism Intelligence (Wikileaks 2011)

International Framework

- First steps: define cyber-war context and scope, evaluate interdependence between CI and vulnerability/risk level (anomalies, interferences, cascade effects). Collect infos from private and public sectors. Creation/coordination of national agencies, development of legislation, cyber-security awareness campaigns
- Bilateral and multilateral initiatives. Many institutions: UN, ITU, OSCE, G8, EU, NATO. UN resolutions since 1998 "Developments in the field of information and telecommunications in the context of international security". Still need to define basic concept of info-security and international principles (1999). "Creation of a global culture of cyber-security and the protection of critical information infrastructures" (2004). UNIDIR (1999, 2008)
- In the past: limited international cooperation followed by end of dialogue. More recently: perspectives for a more open debate (even with different focus). Forum for agreements?

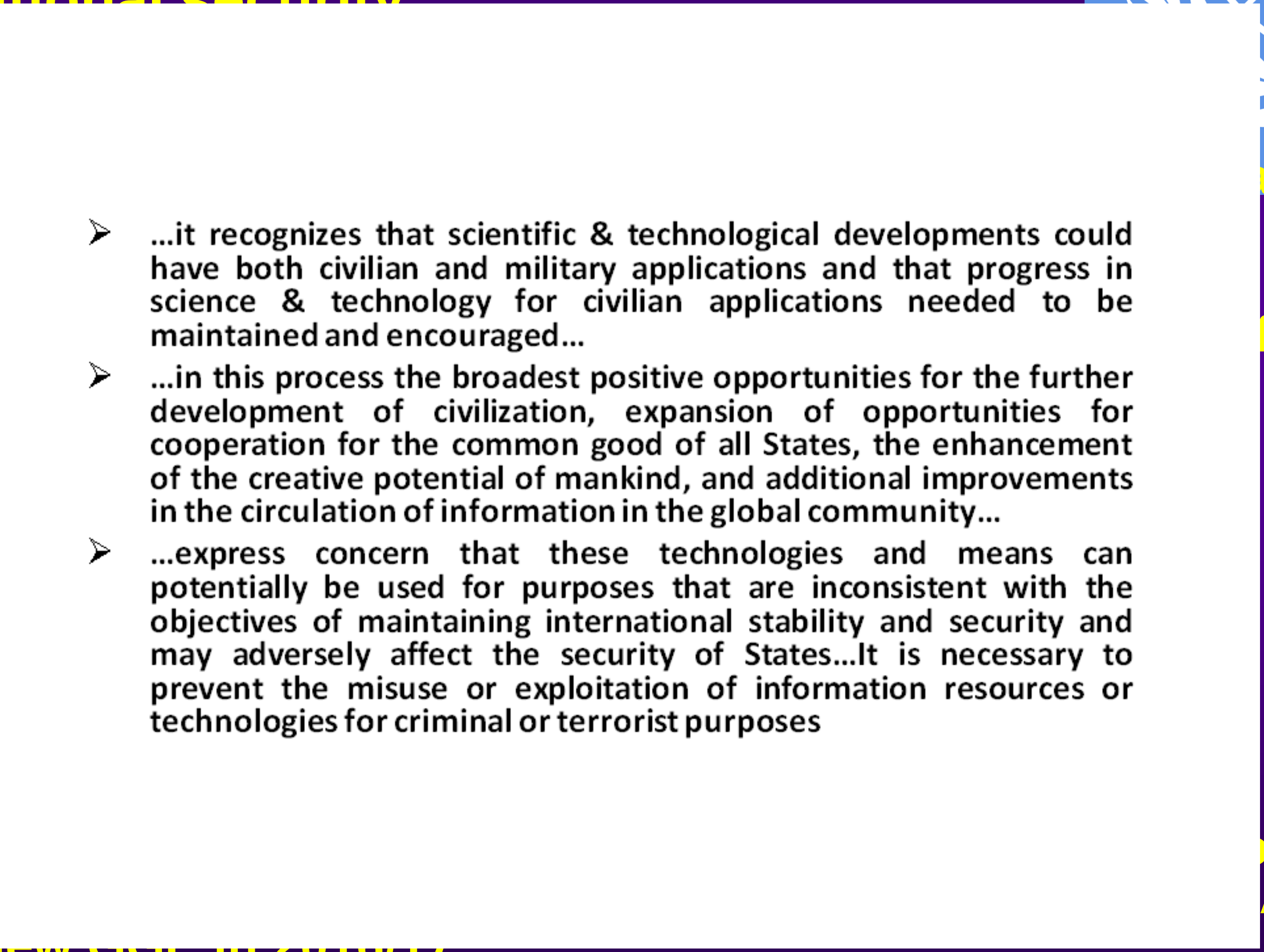
UN agenda

"Developments in the field of information and telecommunications in the context of international security"

Annual

- 2 ambique, N
- 2 Canada, O f Korea, S
- 2
- 2
- 2
- 2
- .. Russia

Four Gr existing potentia operative measur A/70/174 2015). New GGE in 2016/17



- …it recognizes that scientific & technological developments could have both civilian and military applications and that progress in science & technology for civilian applications needed to be maintained and encouraged…
- …in this process the broadest positive opportunities for the further development of civilization, expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of mankind, and additional improvements in the circulation of information in the global community…
- …express concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States…It is necessary to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes

Some initiatives - I

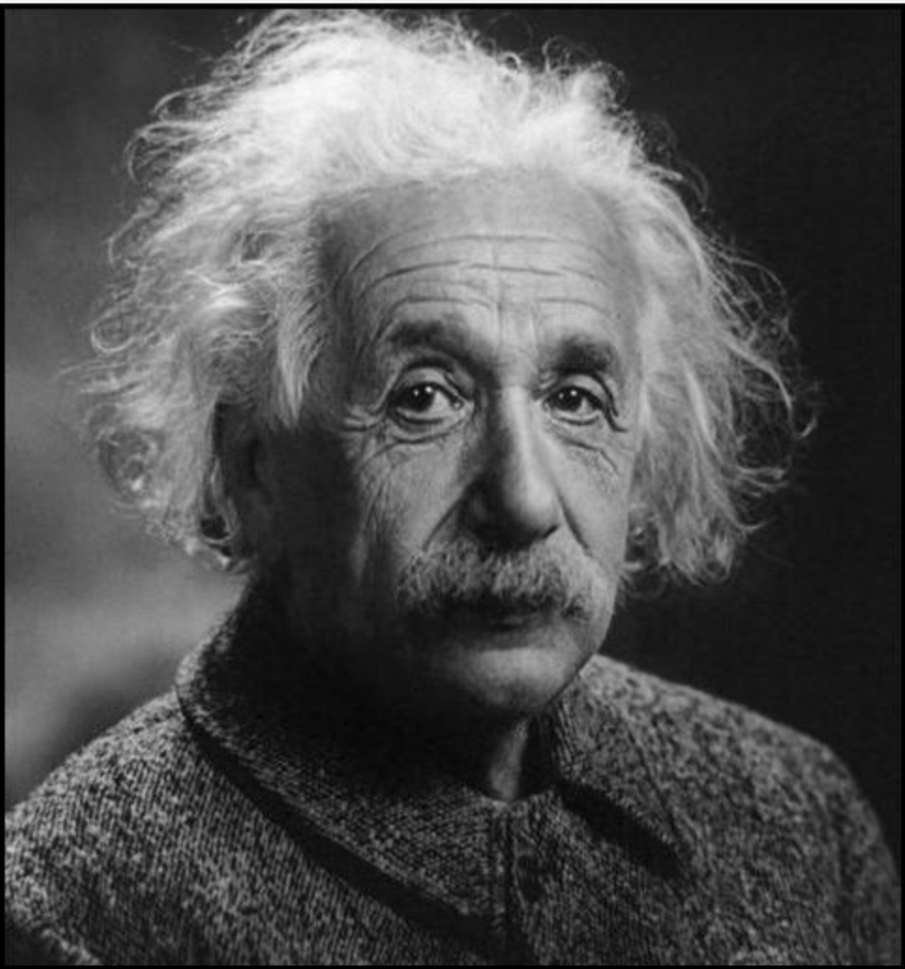
- Trusted identity on the net (nodes, users, processes). Development of mechanisms of authentication, identification, digital certification. Data integrity, confidentiality, availability. Cryptographic techniques. Currently high(?) level of anonymity. Problems(?) with traceback for attribution. Public disclosure of 0-day vulnerabilities? Privacy??
- Creation of international warning centers and support to cyber emergencies/accidents. Distributed sensors (already existing in private world)? Institutions for investigation or/and forensic analysis?
- Effective collaboration/cooperation between public and private sector (diverging interests). Define responsibilities. Pilot programs to define regulations, incentives, political-economic schemes. Resilience

Some initiatives - II

- Cyber-war (technical vision) VS Info-war (content). Privacy, freedom of expression, civil rights
- Development of a clear international legal framework: *jus ad bellum* and *jus in bello*" (discrimination and proportionality, military and civilian targets, neutrality, collateral damages). Is cyber-attack an act of war? Creation of mechanisms to harmonize legal issues in national legislations. Cyber domain probably the least regulated warfare domain (no specific regulation at all) compared to traditional warfare domains (land, air, sea, space)
- Cyber-security: global (asymmetric) issue crossing individual national borders. Total protection impossible. Unavoidable international cooperation?! Collective security!? Global vulnerabilities!!
- At national level: strategic planning to formulate a coherent domestic doctrine. Integration with traditional warfare domains. Coordination of national agencies

Final Notes

- «Cyber universe» new warfare domain, constantly changing environment, artificial, extremely volatile, not well defined. Could it change/reduce the distance among main actors in the international arena, at least partially or temporarily? ≈>40 countries developing cyber offensive capabilities
- Will main military powers dominate also this new dimension? Change balance of power? Asymmetric characteristics may reposition less technologically advanced countries or alter dynamics of global power?
- Future conflicts will have a cyber dimension (hard or soft) currently difficult to evaluate. Number of actors and operational capabilities will increase. Man "in", "on", "out" of the loop. Hostile activities taking place during peace time
- ICT-based approach will not be sufficient: human, organizational, political and economics factors will have to be considered (consequences of outsourcing, deregulation practices, privatization). Cyber supply chain
- Cyber-weapons control?



“The importance of securing international peace was recognized by the really great men of former generations. But the technical advances of our times have turned this ethical postulate into a matter of life and death for civilized mankind today, and made it a moral duty to take an active part in the solution of the problem of peace, a duty which no conscientious man can shirk”